REMARKS

Favorable reconsideration of this application, light of the following discussion, is respectfully requested.

Claims 1-18 are currently pending, with Claims 3-9 and 12-18 withdrawn as directed to non-elected inventions. No claims have been amended herewith.

In the outstanding Office Action, Claims 1, 2, 10, and 11 were rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 5,937,063 to Davis (hereinafter "the '063 patent") in view of U.S. Patent No. 6,938,162 to Nagai et al. (hereinafter "the '162 patent").

Claim 1 is directed to a method for sharing an encrypted data region among two or more processes on a tamper resistant processor having a program and a data encryption and decryption function, the method comprising: (1) giving a common key to each one of the two or more processes; (2) shifting an execution mode of the tamper resistant processor to an encrypted instruction execution mode; (3) operating an owner process among the two or more processes to generate a shared encrypted data region valid only with respect to the common key in a process based on the owner process; (4) operating each of client processes other than the owner process among the two or more processes to map the shared encrypted data region generated by the owner process to a process space of each client process; and (5) setting address information of the shared encrypted data region for each process among the two or more processes in relation to the common key in an encrypted attribute register inside the tamper resistant processor. For a non-limiting example, Applicants refer the Examiner to Figure 4 and the discussion related thereto in the specification.

Regarding the rejection of Claim 1 under 35 U.S.C. § 103, the Office Action asserts that the '063 patent discloses everything in Claim 1 with the exception of the step of setting address information, and relies on the '162 patent to remedy that deficiency.

The '063 patent is directed to a subsystem that prevents the unauthorized replacement of boot-up firmware embedded in a modifiable non-volatile memory device such as flash memory. In particular, the '063 patent discloses that security protection is established by encryption and decryption of the boot-up instructions using a secret key shared by both a secure boot device and a host processor. As shown in Figure 1, the '063 patent discloses that both host processor 50 and secure boot device 54 are configured to contain a shared secret key 64 in respective non-volatile memories 65 and 62. As disclosed by the '063 patent, the shared secret key 64 is established at manufacture during initialization.

Further, the '063 patent discloses that the host processor 50 issues a read request for an address corresponding to the boot-up program (step 110) and the secure boot device detects this boot-up address by having its address space mapped to the corresponding boot-up program (step 112). Next, the '063 patent discloses that the secure boot device 54 encrypts the corresponding boot-up instructions by using the shared secret key 64 (step 114), and the secure boot device responds to the host request with the encrypted boot-up instruction (step 116). Finally, the '063 patent discloses that the host processor 50 decrypts the encrypted boot-up instruction by using the shared secret key 64 (step 118). In step 120, it is determined whether the resulting decrypted boot-up instruction is an improper or invalid instruction. If it is not an invalid instruction, the '063 patent discloses that the host processor 50 proceeds with the next boot-up instruction until the entire booting sequence is completed (step 140).

However, Applicants respectfully submit that the '063 patent fails to disclose the step of operating each of client processes other than the owner process among the two or more processes to map a shared encrypted data region generated by the owner process to a process space of each client process, as recited in Claim 1. Further, it is unclear to Applicants how the '063 patent discloses operating an owner process among the two open processes to generate a shared encrypted data region valid only with respect to the common key in a

process space of the owner process, as recited in Claim 1. Further, Applicants note that Claim 1 is directed to a method for sharing an encrypted data region among two or more processes on a tamper resistant processor, but that the '063 patent is directed to communication between a host processor and a secure boot device over a system bus, as illustrated in '063 Figure 1.

Regarding the step of operating each of client processes other than the owner process among the two or more processes to map shared encrypted data region to a process space of each client process, the Office Action refers to column 3, lines 11-61, and to column 3, lines 34-36 of the '063 patent as disclosing this limitation. In particular, Applicants note that the Office Action asserts that

> [t]he encrypted data region is shared between the secured boot device and a host processor. Processes associated with a host processor request an encrypted boot-up instruction, receive an encrypted boot-up instruction, and map an encrypted boot-up instruction to a process space of a host processor (e.g., column 3, lines 34-36).[1]

However, Applicants respectfully submit that this is not what the '063 patent discloses. As shown in Figure 2, the cited passage in the '063 patent merely disclose that a host processor issues a read request for an address corresponding to the boot-up program, the secure boot device detects a boot-up address, the secure boot device encrypts the associated boot-up instruction using the shared secret key, the secure boot device responds to the host request with the encrypted boot-up instruction, and the host processor decrypts the encrypted boot-up instruction using the shared secret key. *Thus, the '063 patent merely discloses a process of secure communication of boot-up instructions between a boot device and a host processor using encryption and decryption.* However, Applicants respectfully submit that the '063 patent's disclosure that "a secure boot device responds to the host request with the encrypted boot-up instruction" cannot be used to support the Examiner's conclusion that "the encrypted

[1] Page 4 of the outstanding Office Action.

data region is shared between the secured boot device and a host processor," as asserted on page 4 of the outstanding Office Action. An encrypted boot-up instruction sent from one device to another is not an encrypted data region of a process space of an owner process shared between a secure boot device and a host processor. Further, Applicants respectfully submit that the '063 patent fails to disclose mapping a shared encrypted data region generated by an owner processor to a process space of each client process, as recited in Claim 1. In this regard, Applicants believe that the Office Action is equating the disclosed step of decrypting an encrypted boot-up instruction by the host processor as reading on the step of operating each client process other than the owner process among the two or more processes to map the shared encrypted data region generated by the owner process to a process space of each client process, as recited in Claim 1. However, Applicants respectfully submit that decrypting a received instruction by the host processor does not read on operating each of client processes other than the owner process to map a shared encrypted data region generated by the owner process to a process space of each client process. The Office Action has failed to identify which is the claimed client process that does the claimed mapping in the '063 patent. Further, the Office Action has failed to state what is the claimed process space of each client process in the '063 patent.

The '162 patent is directed to a recording type optical disk on which data is recordable, including a data recording and reproducing area for recording data therein and reproducing data therefrom, and a read only disk identification information area for recording disk identification information. However, Applicants respectfully submit that the '162 patent fails to remedy the deficiencies of the '063 patent, as discussed above. The '162 patent does not disclose operating each of client processes other than the owner process among the two or more processes to map the shared encrypted data region generated by the owner process to a

process space of each client process, as recited in amended Claim 1. Rather, the '162 patent is directed to a method of recording an optical disk.

Thus, no matter how the teachings of the '063 and '162 patents are combined, the combination does not teach or suggest either of the operating steps recited in Claim 1. Accordingly, Applicants respectfully submit that a *prima facie* case of obviousness has not been established and the rejection of Claim 1 (and dependent Claim 2) should be withdrawn.

In the outstanding Office Action, the stated motivation for combining the teachings of the '063 and '162 patents is that "doing so makes the system more robust by facilitating data management of the encrypted data region."[2] However, Applicants respectfully submit that the Office Action is simply stating perceived advantages of Applicants' invention as motivation to combination the cited references, without identifying that, without Applicants' specification, one of ordinary skill in the art would even have thought to address the problem. Such hindsight reconstruction of Applicants' invention cannot be used to establish a *prima facie* case of obviousness. In particular, Applicants respectfully submit that merely stating that the suggested combination makes a more robust system is not adequate motivation for one of ordinary skill in the art to make the suggested combination. For this additional reason, Applicants respectfully submit that a *prima facie* case of obviousness has not been established and the rejection of Claim 1 (and dependent 2) should be withdrawn.

Independent Claim 10 recites limitations analogous to the limitations recited in Claim 1. Accordingly, for the reasons stated above for the patentability of Claim 1, Applicants respectfully submit that a *prima facie* case of obviousness has not been established and the rejection of Claim 10 (and dependent Claim 11) should be withdrawn.

Thus, it is respectfully Claims 1, 2, 10, and 11 patentably define over any proper combination of the '063 and '162 patents.

[2] See page 3 of the outstanding Office Action.

Consequently, in view of the present amendment and in light of the above discussion, the outstanding grounds for rejection are believed to have been overcome. The application as amended herewith is believed to be in condition for formal allowance. An early and favorable action to that effect is respectfully requested.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Kurt M. Berger

Eckhard H. Kuesters
Attorney of Record
Registration No. 28,870

Kurt M. Berger, Ph.D.
Registration No. 51,461

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 03/06)

I:\ATTY\KMB\217'S\217811US\217811US-AM DUE 7-26-06.DOC